

What is claimed is:

1. A method of copy protecting media content comprising:

determining whether the media content is designated as copy once;

if the media content is designated as copy once, obtaining an identifier for the

5 media content;

querying a data repository to determine if the identifier is stored therein;

if the identifier is found in the data repository, modifying or disabling a copy
function; and

if the identifier is not found in the data repository, adding the identifier to the data

10 repository.

2. The method of claim 1, wherein the identifier comprises a content identifier.

3. The method of claim 2, wherein the content identifier is conveyed by a digital

15 watermark embedded in the media content, and said obtaining step comprises reading the
digital watermark to obtain the content identifier.

4. The method of claim 2, wherein the content identifier is obtained from a
header associated with the media content.

20

5. The method of claim 2, wherein the content identifier is obtained from an
encryption system associated with the media content.

6. The method of claim 2, wherein the content identifier is obtained by determining a fingerprint of the media content.

7. The method of claim 1, wherein the media content is stored on physical media,
5 and the identifier comprises a physical media identifier.

8. The method of claim 7, wherein the physical media comprises a DVD, and the physical media identifier comprises a unique serial number corresponding to the DVD.

10 9. The method of claim 1, further comprising allowing copying of the media content when the identifier is not found in the data repository.

10. The method of claim 1, wherein the media content comprises a digital watermark embedded therein, the digital watermark indicating that the media content is
15 designated as copy once, and wherein said determining step comprises reading the digital watermark.

11. The method of claim 1, wherein the media content comprises metadata associated therewith, the metadata indicating that the media content is designated as copy
20 once, and wherein said determining step comprises analyzing the metadata.

12. The method of claim 11, wherein the metadata is stored in a file header.

13. The method of claim 1, wherein the media content is associated with an encryption system, the encryption system indicating that the media content is designated
5 as copy once, and wherein said determining step comprises communicating with the encryption system.

14. A recording device performing the method of claim 1.

10 15. The recording device according to claim 14, wherein the data repository is co-located with the recording device.

16. The recording device according to claim 14, wherein the data repository is remotely located from the recording device.

15 17. A recording device that is operable to copy media content, said device comprising:

a data repository;

electronic processing circuitry;

20 a system communications bus to facilitate communication between the data repository and the electronic processing circuitry, said electronic processing circuitry executing steps of:

determining whether media content is designated as copy once;

if the media content is designated as copy once, obtaining an identifier for the media content;

querying the data repository to determine if the identifier is stored therein;

5 if the identifier is stored in the data repository, modifying or disabling a copy function; and

if the identifier is not stored in the data repository, storing the identifier to the data repository.

10 18. A method of providing copy protection for protected media content on a computer system, the computer system comprising an output port and an associated output buffer, and an input port and an associated input buffer, said method comprising:

analyzing first media content buffered in the output buffer;

analyzing second media content buffered in the input buffer; and

15 comparing the first media content buffered in the output buffer with the second media content buffered in the input buffer, wherein a copy operation is modified or disabled when the first media content and the second media content match or otherwise coincide.

20 19. The method of claim 18, wherein the computer system comprises a single computer system.

20. The method of claim 19, wherein the output buffer comprises a matrix of output buffers, and the input buffer comprises a matrix of input buffers.

21. The method of claim 20, wherein said comparing step compares at least
5 active output buffers with active input buffers.

22. The method of claim 18, wherein the computer system comprises at least two networked computers, with a first computer comprising the output port and a second computer comprising the input port.

10 23. The method of claim 22, wherein the output buffer comprises a matrix of output buffers, and the input buffer comprises a matrix of input buffers.

24. The method of claim 23, wherein said comparing step compares at least
15 content buffered in active output buffers with content buffered in active input buffers.

25. The method of claim 18, wherein the first media content comprises a first identifier embedded therein in the form of a digital watermark and the second media content comprises a second identifier embedded therein in the form of a digital
20 watermark, and wherein said step of analyzing first media content buffered in the output buffer comprises obtaining the first identifier from its watermark, said step of analyzing second media content buffered in the input buffer comprises obtaining the second

identifier from its watermark, and said step of comparing the first media content buffered in the output buffer and the second media content buffered in the input buffer comprises comparing at least a portion of the first identifier with at least a portion of the second identifier.

5

26. The method of claim 25, wherein the copy operation is modified or disabled when the portion of the first identifier and the portion of the second identifier match or otherwise coincide.

10

27. The method of claim 18, wherein the first media content comprises a first identifier embedded in the form of a digital watermark, and wherein said step of analyzing first media content buffered in the output buffer comprises obtaining the first identifier from its watermark, and said step of analyzing second media content buffered in the input buffer comprises obtaining a plurality of identifiers embedded as digital watermarks in the second media over a time period, and said step of comparing the first media content buffered in the output buffer and the second media content buffered in the input buffer comprises comparing at least a portion of the first identifier with at least portions of the plurality of identifiers.

15

20


28. The method of claim 27, wherein the copy operation is modified or disables when the portion of the first identifier and the portions of the plurality of identifiers match or otherwise coincide.

29. The method of claim 18, wherein said step of analyzing first media content buffered in the output buffer comprises determining a first fingerprint of the first media content, said step of analyzing second media content buffered in the input buffer comprises determining a second fingerprint of the second media content, and said step of
5 comparing the first media content buffered in the output buffer and the second media content buffered in the input buffer comprises comparing at least a portion of the first fingerprint with at least a portion of the second fingerprint.

30. The method of claim 29, wherein the copy operation is modified or disabled
10 when the portion of the first fingerprint and the portion of the second fingerprint match or otherwise coincide.

31. The method of claim 29, further comprising compensating for a time delay associated with the second media content, relative to the first media content.

15 32. The method of claim 18, further comprising determining that the media content is protected via reference to at least one of a digital watermark, header, metadata and encryption system.



33. A method of providing copy protection for protected media content on a computer system, the computer system comprising an output port and an associated output buffer, and an input port and an associated input buffer, said method comprising:

obtaining first media content buffered in the output buffer;

5 obtaining second media content buffered in the input buffer; and

comparing the first media content buffered in the output buffer and the second media content buffered in the input buffer through correlation of the first media content with the second media content, wherein a copy operation is modified or disabled when the correlation of the first media content and the second media content indicates that the
10 first media content and the second media content match or otherwise coincide.

34. The method of claim 33, wherein the correlation makes use of a transform domain.

15 35. The method of claim 34, wherein the transform domain comprises a Fourier domain.

36. The method of claim 35, wherein the first media content and the second media content each comprise audio.

20

37. The method of claim 33, further comprising compensating for a time delay associated with the second media content relative to the first media content.

38. The method of claim 34, further comprising compensating for a time delay associated with the second media content relative to the first media content.

5 39. A method of providing copy control for protected media content comprising:
selectively determining which out of a plurality of copy control systems applies to
the protected media content; and

controlling the protected media content according to the determined copy control
system.

10 40. The method of claim 39, wherein said protected media content comprises a
digital watermark embedded therein according to a key, and wherein said selectively
determining step determines which out of a plurality of copy control systems applies to
the protected media content based on the key.

15 41. The method of claim 40, wherein the key further designates a copy control
state.

20 42. The method of claim 41, wherein the copy control state comprises at least one
of copy never, copy once, copy freely and copy no more.

43. The method of claim 40, wherein the key indicates at least one of an embedding protocol, a watermark payload encryption scheme, an embedding characteristic, a pseudo-random sequence that is used to embed the watermark, locations within the media content used for watermark embedding, media content features to be modified to effect embedding and semantic meaning of particular features of the media content.

44. The method of claim 40, wherein each of the plurality of copy control systems corresponds to at least one unique key.

45. The method of claim 39, wherein the protected media content comprises a digital watermark embedded therein, the digital watermark comprising a multi-bit payload, and wherein said selectively determining step determines which out of a plurality of copy control systems applies to the protected media content based on at least one bit of the multi-bit payload.

46. The method of claim 45, wherein each of the plurality of copy control systems is associated with a unique sequence of bits.

47. The method of claim 39, wherein the plurality of copy control systems comprises at least one of a DVD system and a conditional access TV system.

48. A method of providing copy control for protected media content, the protected media content comprising a digital watermark embedded therein according to a key, said digital watermark comprising a payload, said method comprising:

5 determining which out of a plurality of copy control states should govern the protected media content by reference to the watermark key;

 determining which out of a plurality of copy control systems the content should be handled by reference to the watermark payload; and

 providing copy control according to the determined copy control state through the
10 determined copy control system.